Conditional Disability Discharge Tracking System

Preliminary Evaluation
of
CDDTS Corrective Action Plan

9/9/2003

Introduction

A security risk assessment[1] was performed on the Conditional Disability Discharge Tracking System (CDDTS) for the Department of Education – Office of Federal Student Aid (FSA). In response, the CDDTS contractor, ACS, and the CDDTS System Security Officer, David Yang, developed a Corrective Action Plan (CAP) to address the findings and observations made during the risk assessment. This document provides comments on the responses provided in the CAP to indicate the current status of each risk assessment finding. The goal is to indicate which items may be considered closed (because they have been appropriately addressed), which items are open but will be addressed by actions described in the CAP, and which items may need further consideration.

Format

The comments below provide a preliminary evaluation of the response to each risk assessment observation in the CDDTS Corrective Action Plan. Observations and findings are identified as in the original risk assessment document. For each observation, the evaluation includes the following sections:

- Observation number (from CDDTS risk assessment)
- Summary of observation (from CDDTS risk assessment)
- Resolution/Planned corrective action (response from CDDTS contractor, in *italics*)
- Comment (evaluation of Corrective Action Plan response)
- Status (current status of corrective actions

Summary

Most of the observations and findings in the CDDTS risk assessment have either been addressed satisfactorily or are in the process of being addressed. A few observations will require additional monitoring, or will require additional updates to the System Security Plan to document changes or controls that were not previously described.

The following table summarizes the current status of the response or corrective actions proposed by the CDDTS contractor. The status descriptions have the following definitions:

- **In progress**: corrective actions are currently in the process of being developed and deployed. When supplied, the expected completion date is listed.
- **Planned**: corrective actions are planned to take place at a future date. The expected date of the planned corrective action is provided.
- **Closed**: The CDDTS risk assessment finding has been adequately addressed and no additional actions or response is suggested at this time.
- **Pending**: Additional steps beyond those described in the response are suggested to satisfactorily address the original risk assessment finding.

[1] Security Risk Assessment for Conditional Disability Discharge Tracking System (CDDTS), Accenture, August 15, 2003, Integration Partner Deliverable 120.2.2

Preliminary Evaluation of CDDTS Corrective Action Plan

Summary of status for corrective actions proposed for CDDTS in response to the risk assessment conducted in August 2003.

Observation Number	Observation Summary	Status of Corrective Action	Expected Completion Date
M1	Security testing of changes is not part of the CDDTS configuration management plan.	In progress	Not supplied
M2	Anti-virus tools are not run on the CDDTS server.	Closed	--
M3	Security training during employee orientation is brief and not documented.	In progress	9/30/2003
M4	Disaster recovery plans have not been tested.	Planned	9/19/2003
M5	Business continuity plans have not been tested.	Planned	9/19/2003
M6	A security training and awareness program has not been fully implemented.	In progress	9/30/2003
M7	Several critical security services are performed for CDDTS by contractor divisions that may be acquired by a third party.	Pending (FSA should continue to monitor the status of security services provided by third parties)	--
M8	Security risk analysis and testing is not included in the configuration management plan.	In progress	10/10/2003
M9	Off-site storage of back-up media and business continuity locations are relatively close to the primary CDDTS Data Center.	Closed	--
O1	Authorized access is not reviewed annually.	Closed	--
T1	Audit trail logging and review are not routinely performed.	In progress	9/19/2003
T2	User passwords for the CDDTS application are stored in clear text.	In progress	9/19/2003
T3	There are no functions to detect and lock accounts after repeated login failure.	In progress	9/19/2003
T4	The System Security Plan does not specify periodic scanning for unauthorized modems.	In progress	9/19/2003
T5	An Intrusion Detection System is not yet fully implemented.	In progress	9/19/2003

T6	Firewall policies and filtering rules should be audited.	Closed	--
T7	CDDTS accounts are not configured for automatic logout after periods of inactivity.	Pending (System Security Plan should be updated)	--
T8	Some file transfers to CDDTS are made through standard FTP.	Pending (System Security Plan should be updated)	--
A1	No CDDTS asset inventory.	Closed	--
A2	A FISMA Privacy Impact Assessment has not been performed.	Pending (A privacy impact assessment should be conducted according to recently published FSA guidelines)	--
A3	The System Security Plan is missing some required content.	In progress	10/10/2003

Comments on CDDTS CAP and Responses to Risk Assessment Observations

---

1. Observation Number: M1

OBSERVATION:
Security testing of changes is not part of the CDDTS configuration management plan.

RESOLUTION/PLANNED CORRECTIVE ACTION:
ACS will revise the CM Plan to incorporate security testing of changes.

The CDDTS servers were scanned for vulnerabilities on 5/22/2003 using vulnerability scanning techniques. Procedures to periodically scan servers for vulnerabilities have been developed and are currently being implemented.

COMMENT:
Development of a procedure for periodic vulnerability scanning will satisfy the requirements for security testing. The procedures should be documented as part of the CDDTS System Security Plan.

STATUS:
In-progress

---

2. Observation Number: M2

OBSERVATION:
Anti-virus tools are not run on the CDDTS server.

RESOLUTION/PLANNED CORRECTIVE ACTION:
Virus Detection software (Norton) has been installed on the CDDTS servers.

Expected completion date: Aug 22, 2003

COMMENT:
Successful deployment of Norton virus scanning software on CDDTS servers will rectify the issue raised in this observation.

STATUS:
Closed

---

3. Observation Number: M3

OBSERVATION:

Security training during employee orientation is brief and not documented.
Proposed countermeasure: Document the security topics covered and the time devoted to them during employee orientation.

RESOLUTION/PLANNED CORRECTIVE ACTION:
Please see response to M6.

COMMENT:
A security awareness training program is being developed to address this finding. The expected completion date is September 30, 2003. The security awareness training program should be evaluated after this date to assess the topics covered in the new employee orientation program and the completeness of the program documentation.

STATUS:
In progress

---

4. Observation Number: M4

OBSERVATION:
Disaster recovery plans have not been tested.

RESOLUTION/PLANNED CORRECTIVE ACTION:
Phase III of CDDTS went live October 31, 2002. ACS will be testing the CDDTS Disaster Recovery plan on September 17, 18 and 19 – within one year of CDDTS being fully functional as planned.

Expected completion date: Sept 19, 2003

COMMENT:
The planned testing of the CDDTS disaster recovery plan should address this finding. The results of the disaster recovery testing should be documented and reported to FSA.

STATUS:
Planned

---

5. Observation Number: M5

OBSERVATION:
Business continuity plans have not been tested.

RESOLUTION/PLANNED CORRECTIVE ACTION:

Phase III of CDDTS went live October 31, 2002. ACS will be testing the CDDTS Business continuity plan on September 17, 18 and 19 – within one year of CDDTS being fully functional as planned.

Expected completion date: Sept 19, 2003

COMMENT:
The planned testing of the CDDTS business continuity plan should address this finding. The results of the business testing should be documented and reported to FSA.

STATUS:
Planned

---

6. Observation Number: M6

OBSERVATION:
A security training and awareness program has not been fully implemented.
Proposed countermeasure: Implement the planned security awareness training program; document the topics covered to demonstrate the effectiveness of the training program; maintain records of training for each user to demonstrate that all users have completed required training.

RESOLUTION/PLANNED CORRECTIVE ACTION:
A security awareness program has been developed. This program will require all employees to undergo Security training through an internal website and compliance will be monitored. All training modules have been developed. The program is currently being rolled out.

Expected completion date: Sept 30, 2003

COMMENT:
A security awareness training program is being developed to address this finding. The expected completion date is September 30, 2003. The security awareness training program should be evaluated after this date to assess the topics covered in the new employee orientation program and the completeness of the program documentation.

STATUS:
In progress

---

7. Observation Number: M7

OBSERVATION:
Several critical security services are performed for CDDTS by contractor divisions that may be acquired by a third party.

RESOLUTION/PLANNED CORRECTIVE ACTION:

ACS presently has an inter-company agreement with ACS Defense to provide security services. This contract can continue after the acquisition of ACS Government Services, Inc. by a third party is completed, if needed. The use of sub-contractor resources to perform certain security services is temporary. ACS is in the process of establishing an alternative to address these security needs.

Expected completion date: N/A

COMMENT:

Security services provided to ACS by third parties should continue to be monitored during periodic CDDTS risk assessments.

STATUS:

In progress

---

8. Observation Number: M8

OBSERVATION:

Security risk analysis and testing is not included in the configuration management plan.

RESOLUTION/PLANNED CORRECTIVE ACTION:

A schedule for periodic risk assessments will be developed for CDDTS and included as part of the Configuration Management Plan (CMP).

Expected completion date: Oct 10, 2003

COMMENT:

Incorporation of plans for periodic risk assessments into the Configuration Management Plan will address this finding. The Configuration Management Plan should be reevaluated during subsequent CDDTS risk assessments.

STATUS:

In progress

---

9. Observation Number: M9

OBSERVATION:

Off-site storage of back-up media and business continuity locations are relatively close to the primary CDDTS Data Center.

RESOLUTION/PLANNED CORRECTIVE ACTION:

ACS has used the current offsite storage (Iron Mountain, Columbia, Maryland) and Disaster Recovery location (Sungard, Philadephia) for the past several years. Careful though has gone into the selection of these facilities. We believe that these facilities are far enough from the Rockville Data Center to allow us to recover from a disaster and are accessible by road in the event of a disaster that prevents air travel.

Expected completion date: N/A

COMMENT:

The use of backup facilities in Columbia, MD and Philadelphia, PA creates the potential that events creating widespread disruption of commercial and infrastructure services will affect both the primary and backup locations. However, the business criticality of the CDDTS system to FSA operations is moderate. Therefore, a business decision to accept the location of the existing backup locations is appropriate when balanced against the additional costs of more remote locations.

STATUS:

Closed

---

10. Observation Number: O1

OBSERVATION:

Authorized access is not reviewed annually.

RESOLUTION/PLANNED CORRECTIVE ACTION:

CDDTS Operating procedure 103 – User Access Authority and Quarterly review of Panagon Access - defines the procedure to be followed to review CDDTS user names on a quarterly basis and to submit to Systems and Networking a list of users that need access removed. A copy of this deliverable is attached.

In addition, ACS has termination procedures that require a terminating employee and the employee's manager to complete a termination checklist and other paperwork on the employee's termination. Part of this process is the notification by the manager to the network administration group to remove all network and system access for the terminating employee.

Expected completion date: N/A

COMMENT:

The documentation provided defines access review procedures that address this observation.

STATUS:

Closed

---

11. Observation Number: T1

OBSERVATION:

Audit trail logging and review are not routinely performed.

RESOLUTION/PLANNED CORRECTIVE ACTION:

Audit logging has been activated on the CDDTS server since May 30, 2003. A written policy to maintain and review audit logs has been developed and approved. We are in the process of implementing this review function.

Expected completion date: Sept 19, 2003

COMMENT:

The activation of audit logging addresses this finding. This issue can be considered closed when the process is in place for reviewing audit log information.

STATUS:

In progress

---

12. Observation Number: T2

OBSERVATION:

User passwords for the CDDTS application are stored in clear text.

RESOLUTION/PLANNED CORRECTIVE ACTION:

The application security module within CDDTS is being enhanced to include a function that will scramble passwords using a hashing algorithm. Logic contained within the same algorithm will be used to convert the password a user provides and match it with the hashed version stored in the CDDTS security tables before allowing the user to proceed with his/her access.

Expected completion date: September 19, 2003

COMMENT:

The recommended application modifications will address the finding, providing that the hashing algorithm conforms to NIST standards.

STATUS:

In progress

---

13. Observation Number: T3

OBSERVATION:

There are no functions to detect and lock accounts after repeated login failure.

RESOLUTION/PLANNED CORRECTIVE ACTION:

The security module within CDDTS is being modified to include functionality to lock accounts after three unsuccessful login attempts. Users will be asked to contact the security administrator to have their passwords reset before they can use the system again.

Expected completion date: September 19, 2003

COMMENT:

The application modification to lock accounts after three unsuccessful login attempts will address the finding. Testing of this functionality should be included in future risk assessments.

STATUS:

In progress

---

14. Observation Number: T4

OBSERVATION:

The System Security Plan does not specify periodic scanning for unauthorized modems.

CORRECTIVE ACTION/DESCRIPTION:

The CDDTS server does not have a modem device installed so unauthorized modem access to the server is not an issue. Scanning for unauthorized modems for PCs that connect to this server will be incorporated as part of the vulnerability scanning procedure.

Expected completion date: Sept 19, 2003

COMMENT:

Adding modem scans to the CDDTS vulnerability scanning procedures will satisfactorily address this finding.

STATUS:

In progress

---

15. Observation Number: T5

OBSERVATION:

An Intrusion Detection System is not yet fully implemented.

RESOLUTION/PLANNED CORRECTIVE ACTION:

1. *Network based IDS (SNORT) was installed on 5/15/2003 on network segments and is currently in use.*

2. *Host intrusion detection software such as Tripwire will be installed on the CDDTS server to detect unauthorized changes to the application and OS components.*

Expected completion date/completion date: Sept 19, 2003

COMMENT:
Implementation of the IDS capability has been initiated but is not yet complete. Tripwire will be installed as part of the CAP to identify unauthorized changes to CDDTS software components. These steps will satisfactorily address the findings in this observation.

STATUS:
In progress

---

16. Observation Number: T6

OBSERVATION:
Firewall policies and filtering rules should be audited.

RESOLUTION/PLANNED CORRECTIVE ACTION:
Firewall policies and filtering rules have been implemented at the Rockville data center where the CDDTS server resides and are available for review.

Expected completion date: N/A

COMMENT:
Firewall policies should be reviewed during security testing planned for CDDTS. No additional actions are required at this time, pending testing and review of the firewall rules that protect the CDDTS network segments.

STATUS:
Closed

---

17. Observation Number: T7

OBSERVATION:
CDDTS accounts are not configured for automatic logout after periods of inactivity.

RESOLUTION/PLANNED CORRECTIVE ACTION:
The CDDTS application currently includes this functionality. The system is programmed to timeout a user after 20 minutes of inactivity. If a user whose session has timed out tries to access the system they get an error message that reads "Your session timed out or you have tried to jump into the system through a bookmark. Please login to the system: Clicking on the "OK" button forces the session to go to the Login page.

Expected completion date: N/A

COMMENT:

This observation was included in the CDDTS risk assessment because the automatic logout functionality was not described in the CDDTS system documentation provided during the risk assessment. A statement that logout functionality is provided should be included in the CDDTS System Security Plan.

STATUS:

Pending

---

18. Observation Number: T8

OBSERVATION:

Some file transfers to CDDTS are made through standard FTP.

RESOLUTION/PLANNED CORRECTIVE ACTION:

The observation identified file transfers between the DLSS and CDDTS servers as unencrypted. DLSS and CDDTS reside at the same location (Rockville data center) on a private network. Access to this network is highly protected by firewalls and routers. These networks also do not have access to an ISP. All access is ACS internal and is controlled by static routing, eventually with access lists. Besides, the FTP process uses complex userids and passwords to access and transfer files. We do not believe this to be a security vulnerability.

Expected completion date: N/A

COMMENT:

The additional protective measures described in this response substantially mitigate risks associated with the use of FTP to transfer files between CDDTS and other systems. The System Security Plan should be updated to include this description of how FTP is used, and the mitigating controls that are in place to protect FTP transfers.

STATUS:

Pending

---

19. Observation Number: A1

OBSERVATION:

No CDDTS asset inventory.

RESOLUTION/PLANNED CORRECTIVE ACTION:

A detailed asset inventory for CDDTS is maintained. Most recently, this inventory was entered into the EDCAS system for the C&A process. The table below lists all CDDTS assets directly *related to CDDTS operations. All assets including the CDDTS servers, components of the NT network, and the LAN are tracked by the ACS Data center inventory control program.*

Asset →	***CDDTS Production server***	***Routers***
Location	*Rockville*	*Rockville*
ID	*CDDTSPRD*	*ATM00 and ATM01*
Manufacturer	*Compaq/HP*	*CISCO*
Model	*DL 380 G2*	*7206 VXR*
IP Address	*172.27.248.60*	*172.21.10.98* *172.21.10.98*
Operating system	*Windows 2000 Advanced Server*	*N/A*
Software installed	• *Oracle 8.1.7 Standard* • *PC Anywhere* • *Network Associates Net-shield* • *IIS*	*N/A*

Expected completion date: N/A

COMMENT:

The information supplied in this response addresses the observation. The system inventory is maintained in the EDCAS system.

STATUS:

Closed

---

20. Observation Number: A2

OBSERVATION:

A FISMA Privacy Impact Assessment has not been performed. .

RESOLUTION/PLANNED CORRECTIVE ACTION:

A FISMA self-assessment for 2003 for CDDTS was completed and submitted to FSA on July, 10, 2003. Prior to this, a GISRA self-assessment was completed and submitted for 2002. ACS awaits feedback on these self-assessments.

Expected completion date: N/A

COMMENT:

This document was not supplied during the risk assessment. A privacy impact statement that follows the recently published Department of Education and FSA guidelines should be prepared and included as part of the system documentation.

STATUS:
Pending

---

21. Observation Number: A3

OBSERVATION:
The System Security Plan is missing some required content.
Proposed countermeasure: Add the Rules of Behavior user agreement and the Memorandum of Understanding to the System Security Plan.

RESOLUTION/PLANNED CORRECTIVE ACTION:

ACS currently requires all employees to read and sign agreements related to proper use of PC software (Employment Agreement – Use of PC Software) and proper use of communication resources (Use of Company Systems/Resources and Information). These agreements cover proper and improper use of computing resources, violation of copyright law, virus protection and software resources.

Rules of Behavior user agreements and Memorandum of Understanding specific to CDDTS will be developed and incorporated as part of the System Security Plan.

Expected completion date: October 10, 2003

COMMENT:
Addition of the identified documentation to the System Security Plan will satisfactorily address this finding.

STATUS:
In progress